8-21-00 A

JC918 U.S. PTO 08/17/00

Please type a plus sign (+) inside this box → [+]

PTO/SB/05 (4/98)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office. U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))

Attorney Docket No.	TIVO0043
First Inventor or Application Identifier	Platt
Title	Drive/Host Locking System
Express Mail Label No.	EL540886091US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents

ADDRESS TO: **Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231**

1. [X] * Fee Transmittal Form *(e.g., PTO/SB/17)* *(Submit an original and a duplicate for fee processing)*
2. [X] Specification [*Total Pages* 20]
   (preferred arrangement set forth below)
   - Descriptive title of the Invention
   - Cross References to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to Microfiche Appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings *(if filed)*
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
3. [X] Drawing(s) *(35 U.S.C. 113)* [*Total Sheets* 4]
4. Oath or Declaration [*Total Pages* 2]
   a. [X] Newly executed (original or copy)
   b. [ ] Copy from a prior application (37 C.F.R. § 1.63(d)) *(for continuation/divisional with Box 16 completed)*
      i. [ ] DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b)

** NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).*

5. [ ] Microfiche Computer Program *(Appendix)*
6. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   a. [ ] Computer Readable Copy
   b. [ ] Paper Copy (identical to computer copy)
   c. [ ] Statement verifying identity of above copies

JC862 U.S. PTO 09/642617 08/17/00

ACCOMPANYING APPLICATION PARTS

7. [X] Assignment Papers (cover sheet & document(s))
8. [X] 37 C.F.R.§3.73(b) Statement *(when there is an assignee)* [X] Power of Attorney
9. [ ] English Translation Document *(if applicable)*
10. [ ] Information Disclosure Statement (IDS)/PTO-1449 [ ] Copies of IDS Citations
11. [ ] Preliminary Amendment
12. [X] Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
13. [X] * Small Entity Statement(s) *(PTO/SB/09-12)* [ ] Statement filed in prior application, Status still proper and desired
14. [ ] Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
15. [ ] Other .....

16. **If a CONTINUING APPLICATION**, *check appropriate box, and supply the requisite information below and in a preliminary amendment*

[ ] Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of prior application No. _____/_____

Prior application information: *Examiner* _____ *Group / Art Unit:* _____

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

[X] *Customer Number or Bar Code Label* 22862 *(Insert Customer No. or Attach bar code label here)* *or* [ ] *Correspondence address below*

Name					
Address					
City		*State*		*Zip Code*	
Country		*Telephone*		*Fax*	

Name (Print/Type)	Michael A. Glenn	*Registration No. (Attorney/Agent)*	30,176
Signature		*Date*	8/17/00

Burden Hour Statement: This form is estimated to take 0.2 hours to complete Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231

Attorney Docket No. TIVO0043

Applicants or Patentees: David PLATT
Serial No.: Unassigned Filing Date: Herewith
Patent No.: Unassigned Issued: Unassigned

For: **DRIVE/HOST LOCKING SYSTEM**

VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS
37 CFR 1.9(f) and 1.27(b) - SMALL BUSINESS CONCERN

I hereby declare that I am:

( ) the owner of the small business concern identified below:

(X) an official of the small business concern empowered to act on behalf of the concern identified below:

NAME OF CONCERN TiVo, Inc.
ADDRESS OF CONCERN 2160 Gold Street, P.O. Box 2160, Alviso, CA 95002-2160

I hereby declare that the above-identified small business concern qualifies as a small business concern as defined in 13 CFR 121.3 - 18 and reproduced in 37 CFR 1.9(c) for purposes of paying reduced fees under Section 41(a) and (b) of Title 35, United States Code, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time, part-time, or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby declare that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention entitled **DRIVE/HOST LOCKING SYSTEM** by inventor(s) David PLATT described in:

(x) the application filed herewith

( ) application serial no. _____, filed _____

( ) patent no. _____, issued _____

If the rights held by the above-identified small business concern are not exclusive, each individual, concern, or organization having rights to the invention is listed below* and no rights to the invention are held by any person, other than an inventor, who could not qualify as a small business concern under 37 CFR 1.9(d), or by any concern that could not qualify as a small business concern under 37 CFR 1.9(d), or a nonprofit organization under 37 CFR 1.9(e).

( ) no such person, concern, or organization
( ) persons, concerns, or organizations listed below*

* NOTE: Separate verified statements are required from each named person, concern, or organization

having rights to the invention averring to their status as small entities (37 CFR 1.27).

FULL NAME _____
ADDRESS _____
( ) INDIVIDUAL ( ) SMALL BUSINESS CONCERN ( ) NONPROFIT ORGANIZATION

FULL NAME _____
ADDRESS _____
( ) INDIVIDUAL ( ) SMALL BUSINESS CONCERN ( ) NONPROFIT ORGANIZATION

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate (37 CFR 1.28(b)).

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

NAME OF PERSON SIGNING James M. Barton
TITLE OF PERSON OTHER THAN OWNER Chief Technical Officer & Vice President Engineering
ADDRESS OF PERSON SIGNING 2160 Gold Street, P.O. Box 2160
Alviso, California 95002-2160

SIGNATURE _____ DATE _____

Attorney Docket No. TIVO0043

Applicants or Patentees: David Platt
Serial No.: _____ Filing Date: Herewith
Patent No.: _____ Issued: _____

VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS
37 CFR 1.9(f) and 1.27(b) - INDEPENDENT INVENTOR

As a below-named inventor, I hereby declare that I qualify as an independent inventor as defined in 37 CFR 1.9(c) for purposes of paying reduced fees under Section 41(a) and (b) of Title 35, United States Code, to the Patent and Trademark Office with regard to the invention entitled:

DRIVE/HOST LOCKING SYSTEM

described in:

(X) the application filed herewith
( ) application serial no. _____, filed _____
( ) patent no. _____, issued _____

I have not assigned, granted, conveyed, or licensed and am under no obligation under contract or law to assign, grant, convey, or license any rights in the invention to any person who could not be classified as an independent inventor under 37 CFR 1.9(c) if that person had made the invention, or to any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(e).

Each person, concern, or organization to which I have assigned, granted, conveyed, or licensed or am under an obligation under contract or law to assign, grant, convey, or license any rights in the invention is listed below:

( ) no such person, concern, or organization

(x) persons, concerns, or organizations listed below*

* NOTE: Separate verified statements are required from each named person, concern, or organization having rights to the invention averring to their status as small entities (37 CFR 1.27).

FULL NAME TiVo, Inc.
ADDRESS 2160 Gold Street, P.O. Box 2160, Alviso, CA 95002
( ) INDIVIDUAL (X) SMALL BUSINESS CONCERN ( ) NONPROFIT ORGANIZATION

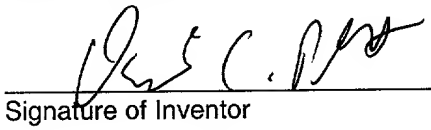
FULL NAME _____
ADDRESS _____
( ) INDIVIDUAL ( ) SMALL BUSINESS CONCERN ( ) NONPROFIT ORGANIZATION

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate (37 CFR 1.28(b)).

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

Attorney Docket No. TIVO0043

Name: David Platt



Signature of Inventor

10 August 2006

Date

DRIVE/HOST LOCKING SYSTEM

This application claims priority from U.S. Patent Application Serial No. 60/160,419 filed October 19,1999.

FIELD OF THE INVENTION

The invention relates to a drive/host locking system which is an authentication system that allows only a desired host to have access to the information stored in a disk drive. More specifically, the invention relates to a system in which this authentication is performed through the use of a password used to unlock the disk drive, thereby providing access to information stored on the disk drive.

DESCRIPTION OF THE RELATED ART

Drive/host locking systems, are known in which a disk drive provides access to a specific host by use of a password security scheme. This type of security system prompts or challenges the host for a password and, once the correct password is supplied, the host gains access to all of the information stored on the disk drive. Using this type of interaction, two authorized computer systems can read and write information between each other in a totally secure environment without the threat of an unwanted host gaining access to the information.

When an outside source or host tries to access the information stored on a locked disk drive, the disk drive asks the host to supply the correct password.

This is also known as challenging the host. If the host supplies the correct password the disk drive becomes unlocked, and the host is allowed full access to all of the information on the disk drive.

To make prior art systems more secure, a system was provided that uses multiple passwords generated by an algorithm implemented by a cryptography circuit. Each password relates to a specific coded challenge asked by the disk drive. These coded challenges are asked at random and only give authorization to the host, which supplies the correct password.

DRIVE HOST

One important aspect of drive/host locking systems is that when the disk drive is not in use, it is locked from all outside sources. When the disk drive challenges a host, and the host supplies the correct password, the disk drive becomes unlocked, giving the host full access to the disk drive. This gives the host the ability to read and write data to and from the drive. Once the host is finished accessing the disk drive, the disk drive is immediately locked again. This step is important in maintaining the security of the drive.

SECURITY AUTHENTICATION PASSWORD

As described above, for a host to gain access to the disk drive the host must be able to supply a correct password. S. Willens, *Network Access Control System and Process,* U.S. Patent No. 5,889,958 (March 30, 1999) demonstrates the importance of using a password to secure a connection between a host and a client computer. However, this type of security does not guarantee the extent of protection necessary to keep the stored information safe from undesired hosts. Eventually, to gain more security, disk drives were designed in which a plurality of challenges are randomly generated, in which only a specific one of the plurality

of passwords from a desired host is allowed, depending on which one of a plurality of challenges is presented by the disk drive. An example of this authentication method is described by D. Platt, S. Lacey, T. Lae, and D. Adams in U.S. Patent Application Serial No. 09/515,408 filed February 29, 2000, Apparatus and Method Capable of Restricting Access to a Data Storage Disk.

With the growing use of technology breaking into coded password protection schemes is easier and much less time consuming. As described in K. Nemoto, *Secure Network Authentication Server Via Dedicated Serial Communication Path*; U.S. Patent No. 6,032,259 (February 29, 2000), it is well known in the art that there is a need for security when connecting between a host and a client computer to prevent invasion from an outside source.

M. Hellman, *Authentication using random challenges*; U.S. Patent No. 5,872,917 (February 16, 1999) also describes using a security method for a host computer accessing a disk drive. However, this authentication method uses multiple transactions between the host and the disk drive making this method very time consuming.

CRYPOTGRAPHY CIRCUIT

Eventually, systems were devised that require the host to prove that it knows the password without actually revealing the password, thus allowing the host to become secretly authorized without any unwanted hosts learning any information about the authorization password. These secret proofs of password knowledge are stored in circuits within the systems. These circuits, also known as cryptographic circuits, are located within the host, and store algorithms for generating the responses needed to authenticate a host secretly. Using a circuit

such as the one described eliminates the host from having any access to the disk drive's information until after it has supplied the correct information to the disk drive.

SUMMARY OF THE INVENTION

Although this proof of password knowledge is a highly reliable security system, it is still not totally secure. Because these codes are pre-set, there is still only a finite number of codes, allowing a very persistent unwanted host, watching and learning, to have the ability to figure out the password.

As a result, yet another stronger form of cryptography was developed. This technique provides a new coded security system between the host and the disk drive, where attempts to break the code and choose the correct password or proof of password knowledge takes longer to learn than the useful life of the disk drive itself. This new coding algorithm between the host and the disk drive proves to be the most secure form of cryptography and is known as SHA-1, or Secure Hash Algorithm.

SHA-1 provides "high security" for the information stored within the disk drive. This algorithm is used by the host to generate complex responses needed to unlock the disk drive. SHA-1 also allows the disk drive and the host to communicate using much larger challenge and responses, making it infeasible to break the password security scheme.

Accordingly, it is an object of the invention to protect the stored information on the disk drive by providing a secure connection between the disk drive and the desired host.

It is another object of the invention to use an authentication system which allows the disk drive to determine if the confronted host is authorized to access the information stored on the disk drive.

It is still another object of the invention to use a password security scheme which allows the disk drive to challenge the host for a password response. This challenge is a challenge value and a lock value generated by the disk drive controller, and is one of a plurality of challenges which is chosen at random. This response is a response value generated by the host using an algorithm which is dependent on both the challenge value and the lock value generated by the disk drive controller.

It is yet another object of the invention to unlock the disk drive for an authorized host and give this host full access to all of the information stored on the disk drive. The disk drive then is locked again after the host has completed accessing the disk drive.

The invention also offers several advantages over previously known authentication schemes, particularly, challenge and response authentication schemes. The security of the authentication, based on the SHA-1 algorithm, is improved to secure completely the information stored on the disk drive, only allowing access to this information by an authorized host.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a flow diagram that illustrates the traditional procedure used when a desired host gains access to a disk drive;

FIG. 2 is a flow diagram that illustrates a new procedure used when a desired host uses the SHA-1 algorithm to gain access to a disk drive according to the invention;

FIG 3 is a block diagram that illustrates communication between the disk drive and the host during authentication according to the invention; and

FIG 4 is a flow diagram that illustrates commands that are used to ensure a secure drive/host locking system according to the invention.

DETAILED DESCRIPTION OF THE INVENTION

A preferred embodiment of the invention and its advantages are better understood by referring to FIGS. 1-4 of the drawings, like numerals being used for like and corresponding parts of the accompanying drawings.

A security feature is provided that uses an authentication password to gain access to the information contained within a disk drive. This access is only granted to a host which can supply the correct password set. This password scheme has been carefully designed so as to never be repeated, therefore making it virtually impossible for an undesired host to gain access to the information stored within the disk drive. This password scheme uses much larger challenges from the disk drive, 512 bits for each challenged value such that it is never necessary to repeat the same challenge within the life span of the disk drive components. Thus, its possible that a single password is never repeated. The password scheme also uses a cryptography circuit for producing the password responses for, and depending on, the disk drive challenges. This technique allows the circuit to provide password response value of, for example 160 bits for each password response value, making it virtually impossible for an

outside source to decipher the password algorithm. This cryptography circuit allows the host and the disk drive to communicate using a key while the disk drive is still locked and before any information is read off the disk drive itself.

BASIC OVERVIEW

The herein disclosed drive/host locking system allows only authorized users to have access to the drive system. This authorization is provided through the use of a disk drive challenge and a host authentication password, as shown in Fig. 1. It is known to have a disk drive locked to secure the valuable information from an outside source **10**. When an outside source, or host, tries to access the information stored on the disk drive **11** the disk drive asks the host to supply the correct password. This is also known as challenging the host **12**. The host then responds by generating a password **13**. If the host supplies the correct password, the disk drive becomes unlocked **14**, and the host is allowed to have access to all of the information on the disk drive **15**. The host now has total access to the disk drive until it is finished accessing the information **16**. Once the host's access to the disk drive's information is complete, the disk drive becomes locked again **17**.

To make this system more secure, it is known to use multiple passwords, where each password relates to a specific coded challenge asked by the disk drive. These coded challenges are asked at random and only give authorization to the host which supplies the correct_password. However, because there are only a finite number of passwords and coded challenges, it was discovered that it is possible for an unwanted host to watch and learn the codes used to access the disk drive and attempt to gain access to the disk drive by continuously trying the learned passwords until one matches with the disk drive's coded challenge.

As a result, a system was devised in which the host proves that it knows the password without actually revealing the password. This allows a host to become

secretly authorized without any unwanted hosts learning any information about the authorization password. These secret proofs of password knowledge are stored in circuits within the personal television device. These circuits, also known as cryptographic circuits, are located within the disk drive, and store the challenges and responses needed to authenticate a host. As in the technique described above, these challenges and response are also chosen at random to secure the system further.

Although this proof of password knowledge is a highly reliable security system, it is still not totally secure. Because these codes are pre-set, there are still only a finite number of codes. This allows a very persistent unwanted host, by watching and learning, to figure out the password.

Referring now to Fig. 2, yet another stronger form of cryptography is shown. This technique provides a new coded security system between the host and the disk drive, where attempts to break the code and choose the correct password or proof of password knowledge take longer to learn than the life to the disk drive itself. This new coding algorithm between the host and the disk drive proves to be the most secure form of cryptography and is known as SHA-1, or Secure Hash Algorithm **23**.

The password is never actually used, only the proof of password knowledge is used and that is enough to prove that the host is allowed to access the information on the disk drive. There is also only a single response to each challenge. The challenge is randomly generated by the disk drive controller, and the response is generated by using the SHA-1 algorithm on the cryptography chip. The disk drive controller is then able to implement the algorithm and verify the response, where this disk drive controller is secretly stored on a portion of the disk drive which is readable by the host, in flash memory or EEPROM.

The time used for this transaction is extremely quick. In the presently preferred embodiment of the invention, only takes a fraction of a second for the disk drive controller to implement the algorithm, and it takes a little over a half of a second for the host to generate the proof of password information.

The next step in this password identification authentication is for the disk drive to boot up unattended and for the host to supply the correct password for access to the disk drive without user intervention. Using this type of interaction, two authorized computer systems can read and write information between each other in a totally secured environment without the threat of an unwanted host gaining access to this information.

SHA-1

This drive/host locking feature is intended to provide a way to marry a disk drive and host computer in a way which makes the drive difficult or impossible to use in any system other than the designated host. This technique is similar in intent to a password scheme, but is significantly more secure.

A basic requirement of the invention is that both the drive controller and the host computer, or some peripheral attached thereto, are capable of storing a small amount of key information, roughly 1024 bits, executing a secure hashing algorithm (SHA-1), generating random numbers, and comparing two values. For adequate security, it is necessary that the key storage, and the calculation of the SHA-1 hash values be performed in a way which prevents the key information from being viewed or copied by an external user. Ideally, these functions are implemented in a physical secure cryptographic module, an integrated circuit or dongle, attached to, or integrated into, the host processor.

The password schemes used by drive/host locking systems are devised for the host to prove that it knows the password without actually revealing the password. This allows a host to become securely authorized without any unwanted hosts learning any information about the authorization password. These secret proofs of password knowledge are stored in circuits within the system. These circuits, also known as cryptographic circuits, are located within the disk drive, and store the challenges and responses need to secretly authenticate a host. As in the technique described above, these challenges and response are also chosen at random to secure the system.

Also, yet another stronger form of cryptography is disclosed. This technique provides a new coded security system between the host and the disk drive, where attempts to break the code and choose the correct password or proof of password knowledge take longer to learn then the life to the disk drive itself. This new coding algorithm between the host and the disk drive proves to be the most secure form of cryptography and is known as SHA-1, or Secure Hash Algorithm.

In SHA-1 cryptography, the host is not allowed any access to any of the disk drives information until the host gains the proper authentication. Also, in the past there were a fixed, or finite, set of challenged values. However, in the SHA-1 cryptography, the challenge values are so large that these challenge values never have to be repeated. This technique allows for an extremely large number of proofs of password knowledge response values.

Figure 3 illustrates the communication between a disk drive and a host. The drive/host system's basic requirement is that both the drive controller and the host computer, or some peripheral attached thereto, are capable of storing a small amount of key information (roughly 1024 bits in the presently preferred embodiment of the invention). On the disk drive **30**, a disk drive controller **31** is

used for generating random challenges and comparing response values. On the host **32**, a cryptography chip **33** is used to XOR challenge and lock information and to run the SHA-1 algorithm on this information to produce a response value. For adequate security, it is necessary that the key storage, and the calculation of the SHA-1 hash values, be performed in a way which prevents the key information from being viewed or copied by an external user.

The first step is for the host to confront the disk drive **34**. Immediately, the disk drive generates a random challenge **35** for the host to prove its authentication. The host then computes the response **36**, or proof of password value, using the SHA-1 algorithm and the cryptograph chip **33**. The chip uses two inputs, the challenge and the lock values (512 bits each). An XOR function, and the SHA-1 algorithm are used to combine these two inputs to generate a 160 bit proof of password response value. Then the disk drive verifies the proof of password response value **37** to determine whether or not the host is allowed access to the information. If the hash values do not match, the drive controller rejects the command, reporting an authentication error to the host. If the hash values do match, the drive controller allows access to the host **38** by unlocking the drive – switching it either to the unlocked for data state (if the data-access key was used) or to the fully unlocked state (if the key-change key was used).

The host computer (or its cryptographic module) must calculate the appropriate authentication response. It does so by choosing one of the two drive keys it knows (data-access or key-change) and computing the value:

A=SHA (challenge XOR key)

The random challenge value and the specified key are XORed in a bit wise fashion, and then are passed as input to the standard SHA-1 Secure Hash Algorithm, described in detail in *Secure Hash Standard,* Federal Information

Processing Standard 180-1, National Institute of Standards and Technology (April 17, 1995). The entirety of which is incorporated herein by reference. The output of the hashing algorithm consists of a 160 bit hash value.

SHA-1 is defined in a way which permits it to accept any number of bits as input. It performs its calculations on one or more blocks of 64 bytes (512 bits). In the normal version of the algorithm, the input data is padded out to a multiple of 512 bits by appending a 1-bit, a variable number of 0-bits, and then a 64-bit field giving the number of bits of input prior to the padding.

If it is desirable to use this standard implementation, then the drive locking algorithm uses keys and random challenge values of 55 bytes (440 bits). These are the largest values which can be processed in one 64 byte SHA-1 input block after the standard padding and length encoding are performed. The appropriate padding and encoded length are appended to the (key XOR challenge) value prior to the calculation of the SHA-1 hash.

It is equally possible to use a slightly nonstandard version of SHA-1, which dispenses with the padding and length encoding. In this algorithm, the keys and random challenge values are 512 bits long, and no padding is performed. This approach is preferable, because it simplifies the implementation slightly. The lack of interoperability between this particular SHA-1 variant and the standard form of SHA should not be an issue.

SHA-1 uses 32 bit fixed point arithmetic internally, and is defined in a way consistent with network byte order, big-endian, representation of integers. If implemented on a little-endian processor (for example, Intel CPUs), it is necessary to byte swap the integer values at the beginning of processing, and to byte swap the resulting 160 bit output value.

Because the SHA-1 algorithm is so complex, there is no need to abort the authentication process from a specific host. For example, there is no need to abort the authentication process if a specific host generates three wrong passwords.

COMMANDS

Referring now to Fig. 4, the preferred embodiment of the invention adds three new commands: SET LOCK, REQUEST CHALLENGE, and AUTHENTICATE.

The SET LOCK command **40** is used to set or clear either the drive-access of key-change key. The key being set or cleared is identified by a single bit in one of the IDE drive control registers, *e.g.* LSB of the head number. The command expects to receive one sector (512 bytes) of data through the IDE data FIFO. Only the first 512 bits of this data are significant; the remaining bits are reserved and must be zero. This command is accepted only if the drive is fully unlocked. The drive controller stores the 512-bit key in a reserved area of the disk.

When the drive is powered up or reset it checks the two 512-bit keys. If both of the keys are zero (all 0 bits), the drive is placed in locked state. If either key is nonzero, the drive is placed in the locked state. The drive also generates a 512-bit random number, and stores this random number in some convenient location.

When the drive is in a locked state, the host computer must issue a REQUEST CHALLENGE command **41**. This command causes the drive controller to return one sector (512 bytes) of data containing the 512-bit random number calculated at power-up/reset padded out to 512 bytes with zeros.

The host computer now issues an AUTHENTICATE command **42**. It identified the key it used to calculate the hash value (again, using one bit in one of the IDE

drive control registers) and writes one sector (512 bytes) of data through the IDE and DIDO. This sector of data consists of the 20 bytes (160 bits) of SHA-1 hash valued, padded out with zero byes.

The drive controller retrieves its copy of the key specified by the host and performs the same SHA-1 calculation described above. It then compares the hash value it calculated with the hash value contained in the data sent by the host in the AUTHENTICATE command 42. If the hash values do not match, the drive controller rejects the command, reporting an authentication error to the host. If the hash values do match, the drive controller unlocks the drive, switching it either to the unlocked for data state (if the data-access key was used) or to the fully unlocked state (if the key-change key was used).

KEYS

The preferred embodiment of the invention creates a pair of keys that are known to the drive controller and to the host's cryptographic module. This first key is used to gain access to the drive; the second is used to gain the right to change the keys. At any given moment, the drive is in one of three states: locked (contents cannot be read or written and the keys cannot be changed), unlocked for data (contents can be read and written, but the keys cannot be changed), or fully unlocked (contents can be read and written, and the keys can be changed). If the drive is in the locked state, all commands intended to read and write data to/from the drive are rejected.

There are two keys used in this device both used to unlock and lock the disk drive. The first key is known as the functionality key. The functionality key is located in the receiver's chip and is used to unlock the disk drive when the disk drive challenges the host and the host supplies the correct password. The second key is the master key, or skeleton key. This key is not found within the

receiver's chip. It is kept only with the products designers and programmers. The skeleton key is used to manually unlock and/or lock the disk drive. This is used in instances when the programmer needs to access the disk drive to enter or change information specific to the individual disk drive. This is used on disk drives that either need to be specially modified, upgraded, or need special trouble shooting.

Although the invention is described herein with reference to the preferred embodiment, one skilled in the art will readily appreciate that other applications may be substituted for those set forth herein without departing from the spirit and scope of the present invention. Accordingly, the invention should only be limited by the claims included below.

CLAIMS

1. A method for providing access between a first party and a second party, said method comprising the steps of:

generating a challenge value and a lock value at said first party;

transmitting said challenge to said second party;

generating a response value from said second party;

transmitting said response value to said first party; and

validating said response value by said first party.

2. The method of Claim 1, wherein said first party is a disk drive and said second party is a host computer.

3. The method of Claim 2, wherein said disk drive is locked when not accessed.

4. The method of Claim 3, wherein said step of generating a said challenge value and said lock value further includes the step of using 512 bits for said challenge value and using 512 bits for said lock value.

5. The method of Claim 4, wherein said step of generating a said challenge value and said lock value further includes the step of randomly generating each said challenge value.

6. The method of Claim 5, wherein said step of generating a said challenge value and said lock value further includes the step of using a disk drive controller to generate said challenge value.

7. The method of Claim 6, wherein said step of generating a said response value further includes the step of using an exclusive OR (XOR) to combine the said challenge and said lock values.

8. The method of Claim 7, wherein said step of generating a said response value further includes the step of using 160 bits for said response value.

9. The method of Claim 8, wherein said step of generating a said response value further includes the step of using a cryptography circuit to generate said response value.

10. The method of Claim 9, wherein said step of generating a said response value further includes the step of using an algorithm to generate said response value.

11. The method of Claim 10, wherein said step of generating a said response value further includes the step of using a secure hash algorithm to generate said response value.

12. The method of Claim 11, wherein said step of validating said response value further includes the step of said disk drive controller receiving the challenge and lock values, computing a duplicate response value by performing a duplicate said secure hash algorithm, and comparing the original said response value to the duplicate said response value.

13. The method of Claim 12, wherein said step of validating said response value further includes the step of unlocking the disk drive if the response and duplicate response values match.

14. An apparatus for providing access between a first party and a second party, said apparatus comprising:

means for generating a challenge value and a lock value at said first party;

means for transmitting said challenge to said second party;

means for generating a response value fat said second party;

means for transmitting said response value to said first party; and

means for validating said response value by said first party.

15. The apparatus of Claim 14, wherein said first party is a disk drive and said second party is a host computer.

16. The apparatus of Claim 15, wherein said disk drive is locked when not accessed.

17. The apparatus of Claim 16, wherein said means for generating a said challenge value and said lock value further includes using 512 bits for said challenge value and using 512 bits for said lock value.

18. The apparatus of Claim 17, wherein said means for generating a said challenge value and said lock value further includes means for randomly generating each said challenge value.

19. The apparatus of Claim 18, wherein said means for generating a said challenge value and said lock value further includes means for using a disk drive controller to generate said challenge value.

20. The apparatus of Claim 19, wherein said means for generating a said response value further includes an exclusive OR (XOR) for combining the said challenge and said lock values.

21. The apparatus of Claim 20, wherein said means for generating a said response value further includes using 160 bits for said response value.

22. The apparatus of Claim 21, wherein said means for generating a said response value further includes a cryptography circuit for generating said response value.

23. The apparatus of Claim 22, wherein said means for generating a said response value further includes an algorithm for generating said response value.

24. The apparatus of Claim 23, wherein said means for generating a said response value further includes a secure hash algorithm for generating said response value.

25. The apparatus of Claim 24, wherein said means for validating said response value further includes a means for said disk drive controller receiving challenge and lock values, computing a duplicate response value by performing a duplicate said secure hash algorithm, and comparing the original said response value to the duplicate said response value.

26. The apparatus of Claim 25, wherein said means for validating said response value further includes means for unlocking the disk drive if the response and duplicate response values match.

Drive/Host Locking System

ABSTRACT

An authentication system for securing information within a disk drive to be read and written to only by a specific host computer such that it is difficult or impossible to access the drive by any system other than a designated host is disclosed. While the invention is similar in intent to a password scheme, it significantly more secure. The invention thus provides a secure environment for important information stored within a disk drive. The information can only be accessed by a host if the host can respond to random challenges asked by the disk drive. The host's responses are generated using a cryptography chip processing a specific algorithm. This technique allows the disk drive and the host to communicate using a coded security system where attempts to break the code and choose the correct password take longer to learn than the useful life of the disk drive itself.

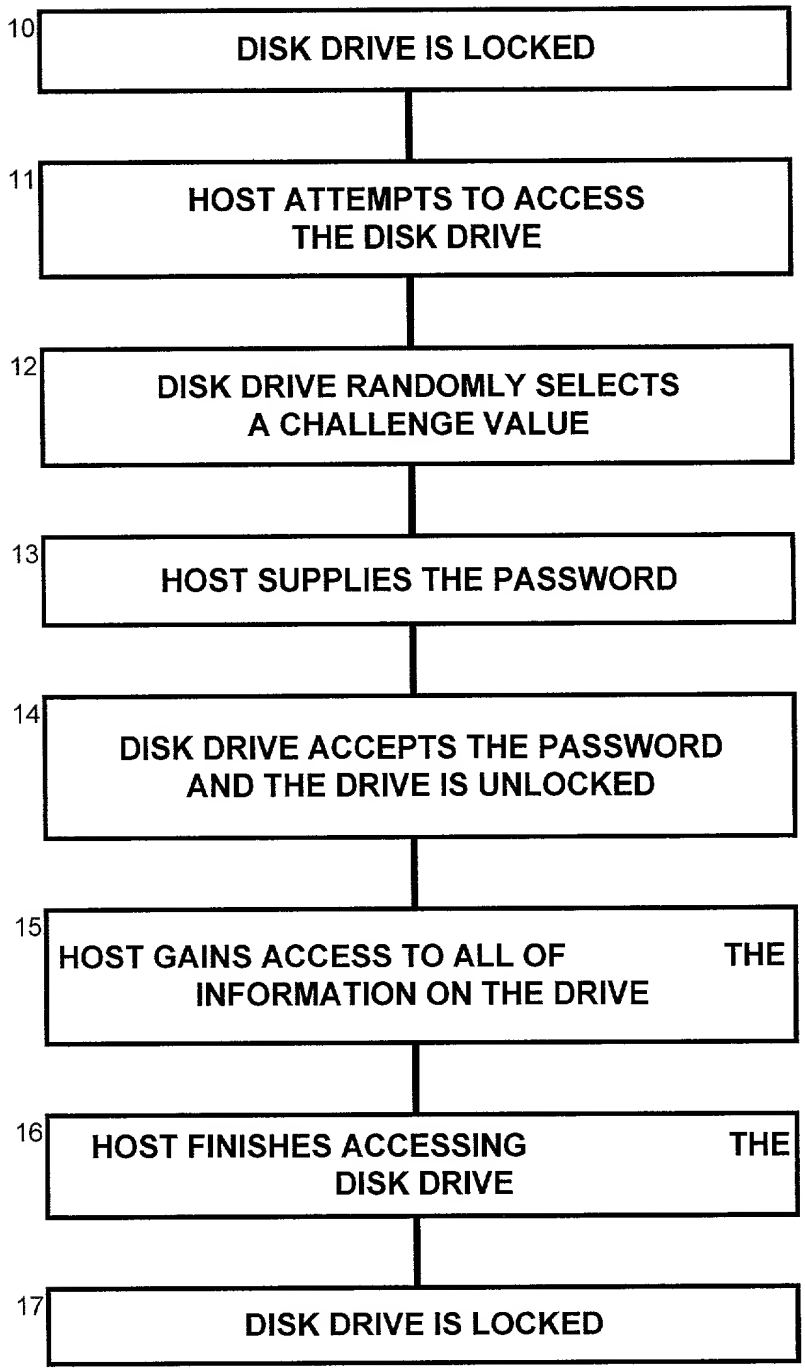


FIG 1 (PRIOR ART)

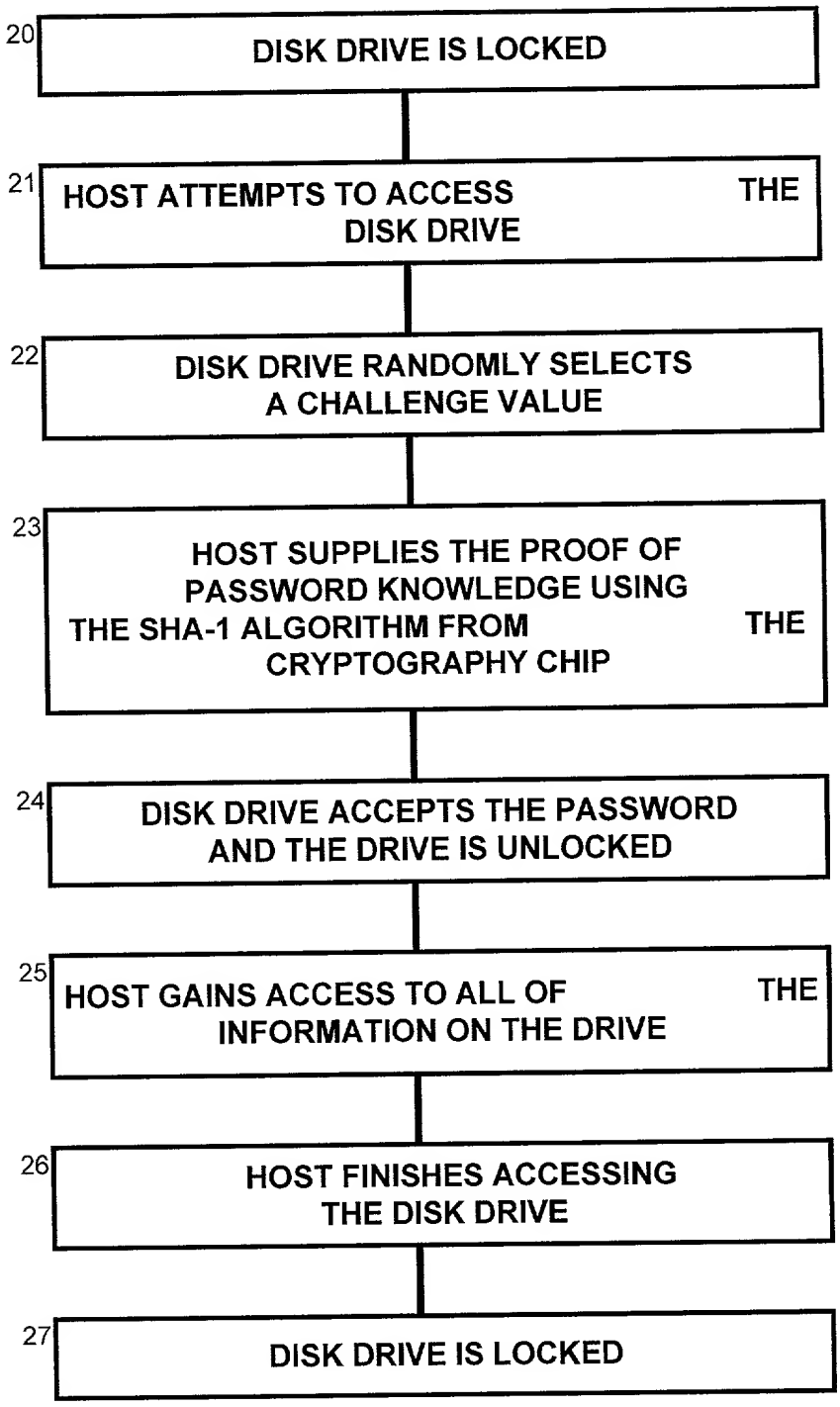


FIG 2

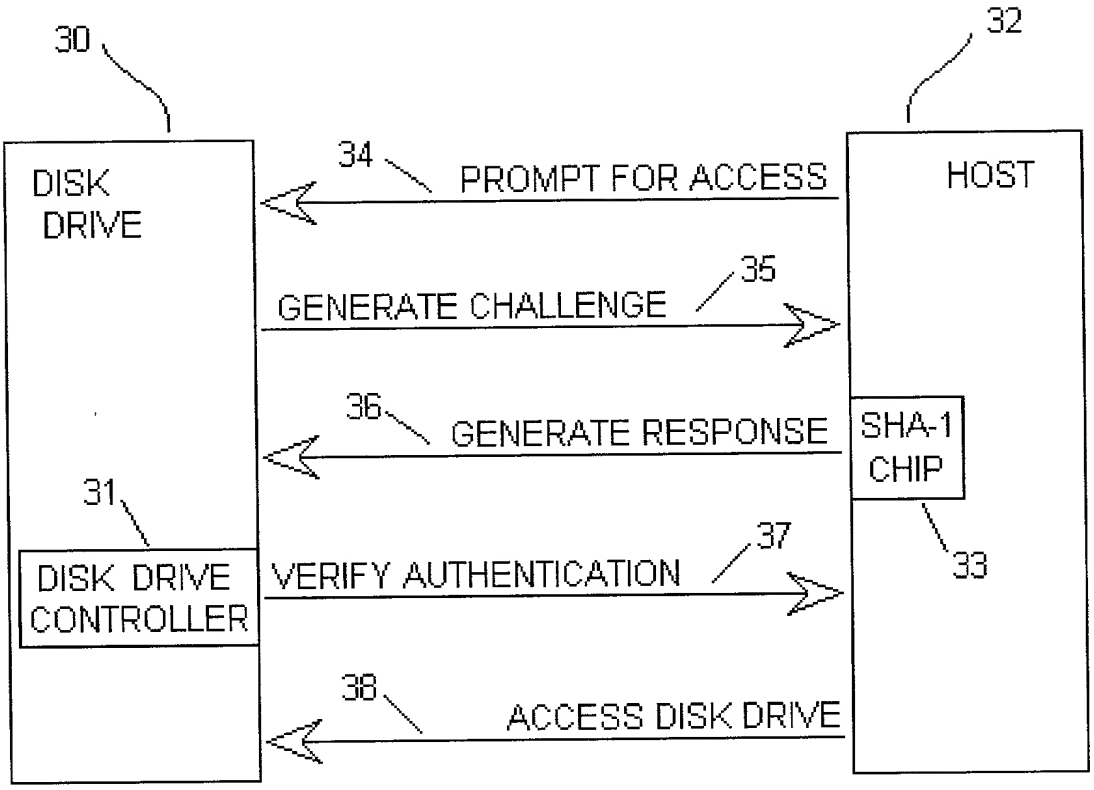


FIG 3

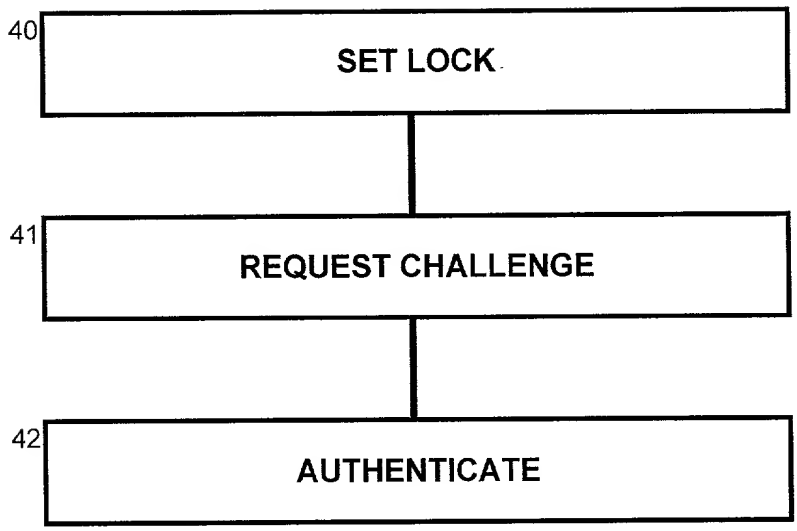


FIG 4

Attorney Docket No. TIVO0043

DECLARATION FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name;

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

DRIVE/HOST LOCKING SYSTEM

the specification of which (check one) _X_ is attached hereto, or __ was filed on _____ as Application Serial No. _____and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56(a).

==========

I hereby claim foreign priority benefits under Title 35, United Sates Code, Section 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)	Priority Claimed Yes	No
_____ Number Country Day/Month/Year Filed	____	____
_____ Number Country Day/Month/Year Filed	____	____

==========

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith:

MICHAEL A. GLENN, Reg. No. 30,176
DONALD M. HENDRICKS, Reg. No. 40,355
KIRK D. WONG, Reg. No. 43,284
EARLE W. JENNINGS, Reg. No. 44,804
CHRISTOPHER PEIL, Reg. No. 45,005

SEND CORRESPONDENCE TO:

MICHAEL A. GLENN, 3475 Edison Way, Suite L, Menlo Park, CA 94025

==========

Attorney Docket No. TIVO0043

I hereby claim the benefit under Title 35, United States code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, Section 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Application Ser. No.	Filing Date	Status: Patented, Pending, Abandoned
Application Ser. No.	Filing Date	Status: Patented, Pending, Abandoned

==========

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of first or sole inventor: DAVID PLATT

Inventor's signature _____ 26 July 2000
Date

Residence 323 Aldean Avenue, Mountain View, California 94043

Post Office Address Same

Citizenship United States of America